	A	B
3	Name	Poster #
4	J. Yin	1
5	T. Sobers	2
6	M. Dong	3
7	K. Hu	4
8	H. Wang	5
9	A. Shanmugan	6
10	A. Sheikholeslami	7
11	H. Cai	8
12	T. Teixeira	9
13	Z. Yang	10
14	D. Mo	11
15	S. Feng	12
16	K. Fu	13
17	Y. Lei	14
18	H-C. Chang	15
19	B. Spring	16
20	M. Upadhyaya	17
21	M. Ghadiri-Sadrabadi	18
22	P. Ravindran	29
23	X. Xu	20
24	A. Saranathan	21
25	S. Subramanya	22

UMassAmherst

OrthCredential: A New Network Capability Design for High-Performance Access Control

Hao Cai, Advisor: Prof. Tilman Wolf

Motivation

- In Internet, network services (e.g., packet processing operations) requires access control to ensure that only the users who paid for these services can use them.
- Most of current authentication schemes (cryptographic techniques) have high security but with high cost.
- Design a new authentication mechanism that satisfies "high enough" security and with low cost.

Technical Approach

- The main idea of OrthCredential (Orthogonal Credential) is that the user uses a sequence (credential) which is orthogonal to the verifier's sequences.
- The verifier checks the *inner product* of the user's credential and the sequence on the verifier. The result of the inner product equals 0 means the credential is valid.
- Inner production can be achieved by bitwise operations which are cheap in CPU; the verifier only needs to save a sum of received credentials to prevent replay packets.
- These orthogonal sequences can be easily constructed from a Hadamard matrix.

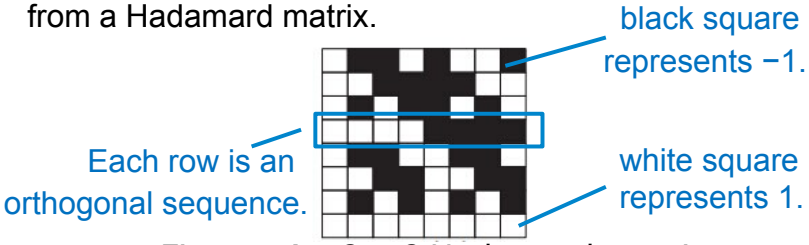


Figure: An *8 x 8* Hadamard matrix.

Results

- Low verification time: 450 cycles per packet guarantee less than 10e-8 success probability of a random attack packet.
- Powerful DoS (Denial of Service) attack defense: less than 50 clock cycles.
- Low Memory Consumption: a space of no more than 0.1 KB on the verifier can promise 10e-8 success probability of a random attack packet while preventing replay attacks simultaneously.
- Small Overhead in Packets: no more than 28 bytes.

Algorithm	Verification time/Packet
HMAC (MD5)	5,335
HMAC (SHA-1)	8,931
AES/CTR (128-bit key)	7,277
DES/CTR	27,350
DMAC (AES)	12,223
OrthCredential	<1000

Table: Comparision with some cryptographic techniques.

Conclusion and Future Work

- We propose a novel design for data plane credential in Internet, which enables access control and can be generated and verified at high data rates with low processing overhead and low storage requirements.
- In the future, we hope to use OrthCredential in path verification of packets in Internet.

UMassAmherst

Bandwidth Limitation of Infinite Planar Phased Arrays in Free Space

Hsieh-Chi Chang, Advisor: Prof. Do-Hoon Kwon

Motivation

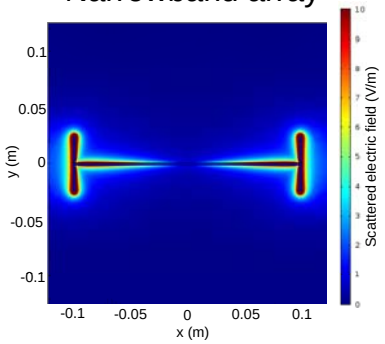
- The bandwidth limitation of an arbitrary free space planar array is not well known
- There is a great interest in wideband and ultrawideband phased array antennas – widest bandwidth using a low-profile structure
- Recent advance in broadband arrays does not provide systematic design approach to meet requirements.

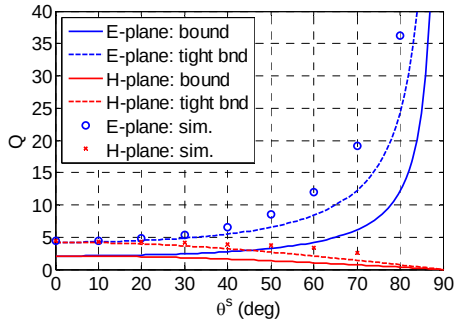
Technical Approach

- Find optical theorem for periodic scatterers
  - Formulate and treat a scattering problem
  - σ_{ext} is an established analytic quantity in complex-k plane
  - Other analytic quantity may also be used
- Find integral identity for scattering area
  - Analyticity of $\rho(k)$ permits a simple integral identity
  - Apply Cauchy theorem to closed contour including Re-k axis
  - Analyze static scattering of element under PEC
- Translate to bandwidth limitation
  - Use $\sigma_{\text{ext}} \geq \sigma_{\text{a}}$
  - Relate σ_{a} to unit cell area, scan angle, and antenna port
  - Inspect elec. & mech. contributions of the upper bound

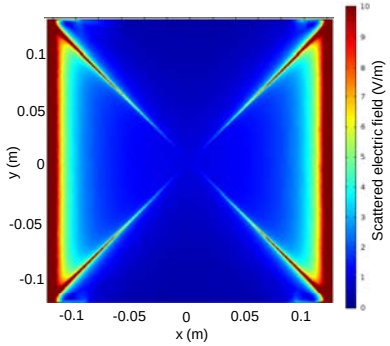
Results

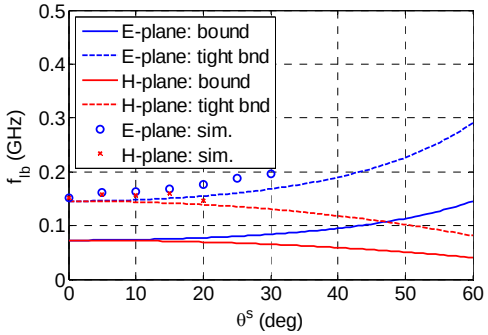
- Narrowband array





- Ultrawideband array





Conclusion

- Provide a valuable insight for designing broadband/wideband arrays
- The bound is expressed in terms of the radiation efficiency, the element Floquet directivity, the projected area of the unit cell and, the strengths of the induced dipole moments.

UMassAmherst

Time Selective Sampling Receivers for Interference Rejection

Minghao, Advisor: Prof. Jackson

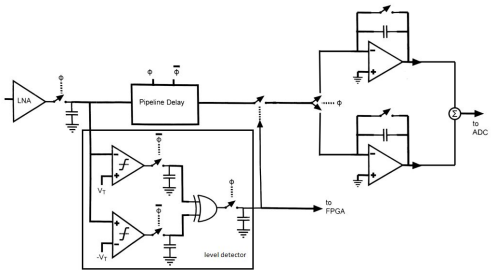
Motivation

- The unique sensing scheme of Cognitive Radios (CR) requires a high instantaneous dynamic range over a wide frequency range, however faces large interferences that may easily desensitize the receiver.
- Our project designed a sample-selecting receiver. Interference rejection can be achieved by retaining only small amplitude samples and discard large distorted samples.

Technical Approach

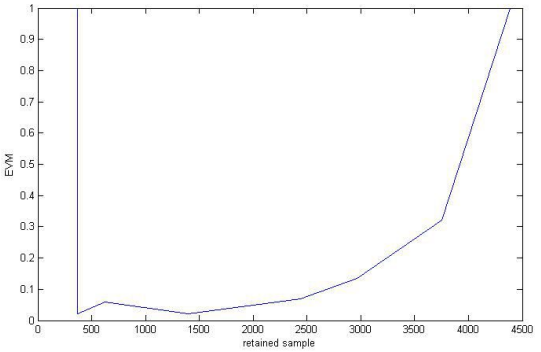
- Challenge: If the frequency of the message is $2\omega_1 - \omega_2$ while two strong interference at frequencie ω_1 and ω_2, the 3rd order side band of interferences may cover the message.

- Solution: Sample the LNA output and keep only samples below some threshold level. Larger samples are distorted.



system block diagram

Results



EVM for different number of samples

(message is 50dB smaller than the interferences, 5000 samples in total)

- Error Vector Magnitude (EVM): $EVM = \frac{|V_{rec} - V_{ref}|}{|V_{ref}|}$ where V_{ref} is the reconstructed message's complex amplitude when there is no interference.

Conclusion: Number of good samples is crucial. Ideal ratio is from 10% to 30% of total samples.

Future Work

- Future work:Increase sampling frequency from 2GHz to 5GHz.

UMassAmherst

TAILORING NON-HOMOGENEOUS MARKOV CHAIN WAVELET MODELS FOR HYPERSPECTRAL SIGNATURE CLASSIFICATION

Siwei Feng, Advisor: Prof. Marco F. Duarte

Motivation

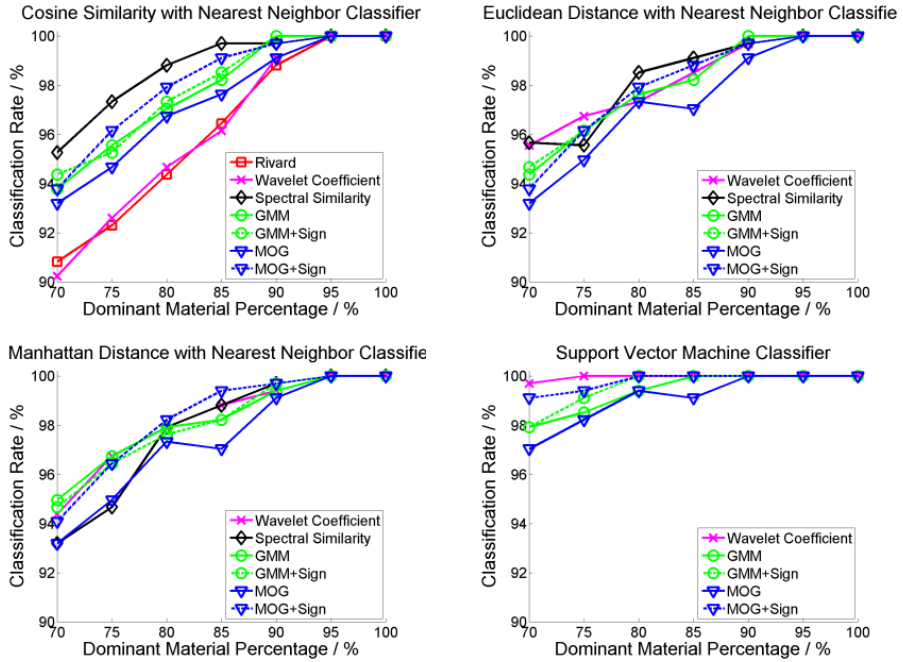
- Improvements in hyperspectral imaging systems bring massive amounts of high-dimensional data.
- Feature extraction is needed but always performed manually
- We focus on the facilitation of information extraction

Technical Approach

- **Wavelet coefficients** act as “detectors” of fluctuations in hyperspectral signatures.
  - **Undecimated wavelet transform** for wavelet analysis
  - **Haar wavelet** as mother wavelet function
  - Final representation: 2-D wavelet array. Rows: scales; columns: offsets/wavelengths.
- **Non-homogeneous hidden Markov chain (NHMC)** model for extracting scientifically meaningful information on the spectral signatures.
  - **Gaussian mixture model (GMM)** for wavelet coefficient characterization
  - **EM algorithm** for GMM parameter training
- **Viterbi algorithm** for generating state labels

Results

- Database: RELAB spectral database including only mineral spectra including 1690 samples from 26 classes.



Conclusion and Future Work

- Explore the influence brought by our feature extraction scheme on classification performance
- Try more feature extraction schemes like using non-zero mean Gaussian mixture model

UMassAmherst

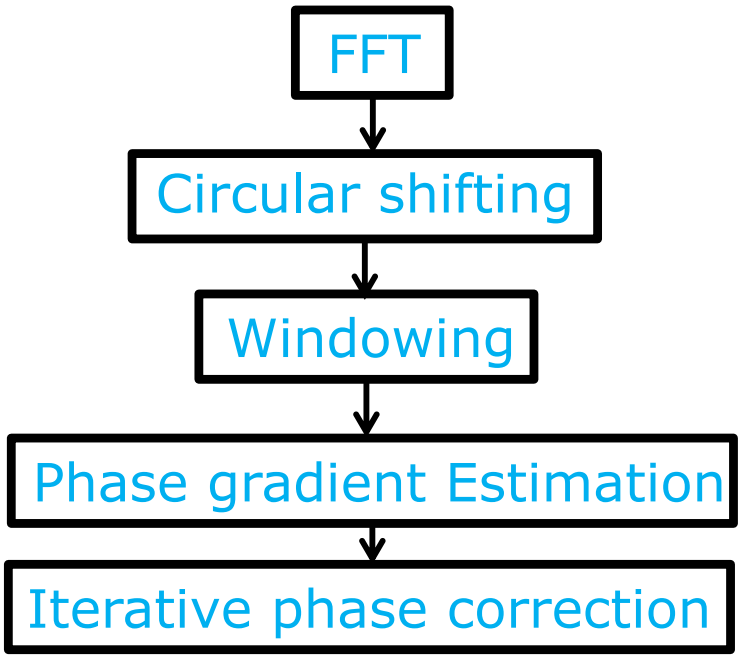
35 GHz Airborne InSAR Processing and Analysis

Kan Fu, Advisor: Prof. Paul R. Siqueira

Motivation

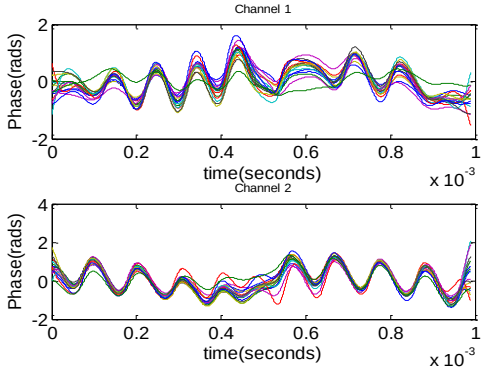
- An airborne interferometric synthetic aperture radar (SAR) radar working at Ka-band(35GHz) was built. 20GB data were recorded during the a flight over western Mass. To improve the accuracy of topography measurement, phase nonlinearities canceling and motion compensation need to be taken in addition to the traditional processing technique. The terrain topography was derived from the InSAR data.

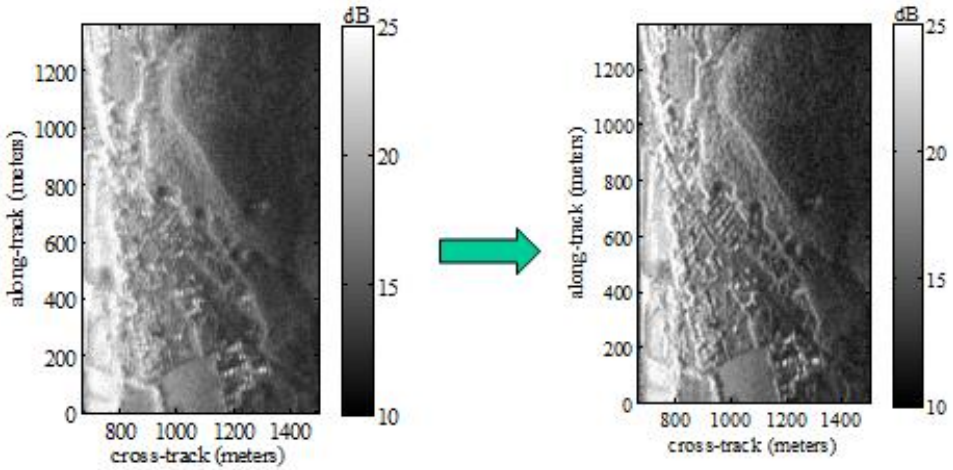
Technical Approach



Results

estimated nonlinear phase error





Conclusion and Future Work

SAR and InSAR images were created after phase nonlinearities canceling and motion compensation. In the future, a quantitatively analysis of the platform motion effects , including the antenna phase center deviation and the signal amplitude variations.

UMassAmherst

mm-Wave Direct Conversion Receiver for In-Situ Noise and Gain Measurements Applications

Mohammad Ghadiri-Sadrabadi, Joseph Bardin

Motivation

- CMOS transistors (with gate lengths below 90 nm) with $ft/fmax$ in the order of 100s of GHz have attracted significant attention to be used for mm-wave applications.
- Large variations in device parameters for CMOS transistors become significant and can affect the performance of the fabricated chip. To overcome this issue, self-optimizing techniques can be used to evaluate the performance of the IC and then tune different parts to achieve the desired performance.

Technical Approach

- In this project a new technique is presented to enable on-chip noise and gain measurements of a DUT at frequencies between 10-20 GHz. For both measurements, there needs to be a sophisticated receiver system that down converts the high frequency signal to an intermediate frequency (IF) for further baseband processing.

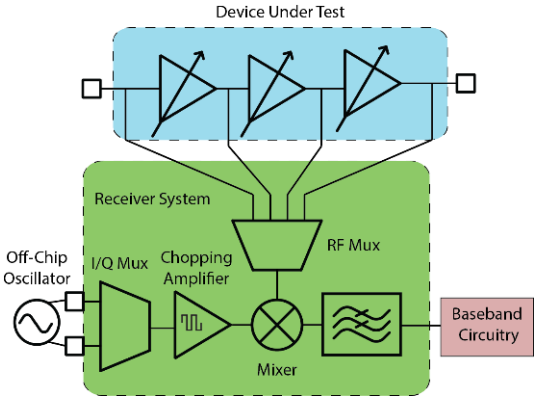


Figure1. Schematic diagram of the complete system on chip

Results

- System was implemented and fabricated in IBM 32nm SOI CMOS.
- Simulation results show 16 dB of conversion gain and 12 dB DSB NF for the receiver system
- Measurements for this project are still ongoing but some promising initial results are presented here

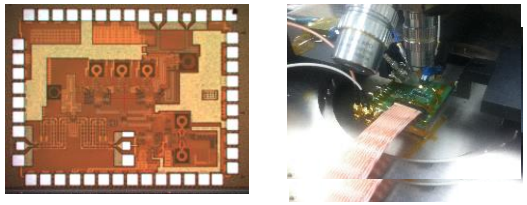


Figure4. Die photo of the 32nm chip and measurement setup for mm-wave receiver testing

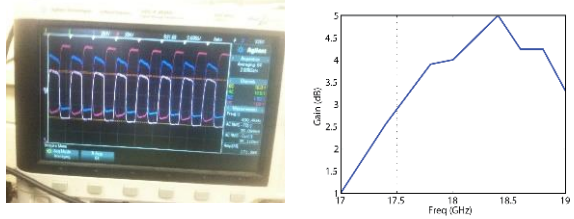


Figure5. Transient response of the amplified receiver output and an example measurement of the gain of one stage of the LNA

Conclusion and Future Work

- Initial measurements of the gain measurement technique show promising results.
- Future work should include the demonstration of the gain measurement with the on chip receiver system.

UMassAmherst

System-Level Security for Network Processors with Hardware Monitors

Kekai Hu, Advisor: Prof. Tessier

Motivation

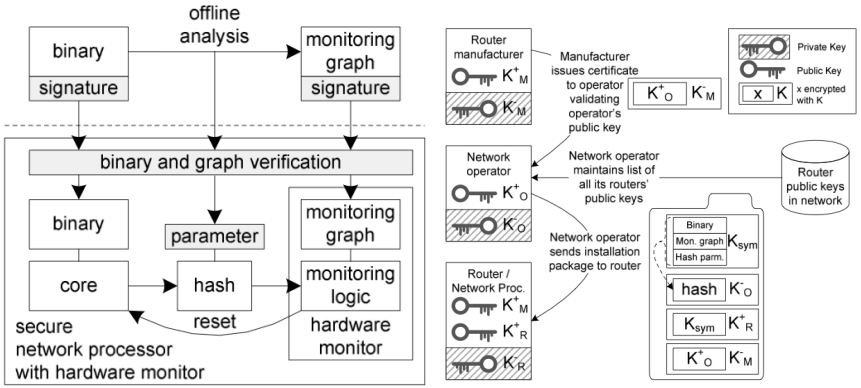
- Network processors with software vulnerability can be attacked by malicious packets.
- Hardware monitors are designed to protect the NPs.

System level challenges:

- Dynamics: Runtime reconfiguration of the network processors and corresponding monitors.
- Homogeneity: Large number of identical devices can be attacked by one attack.

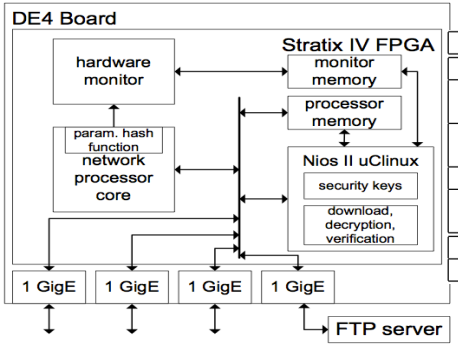
Technical Approach

- Secure Dynamic Multicore Hardware Monitoring System (SDMMon)
- Secure Key Management



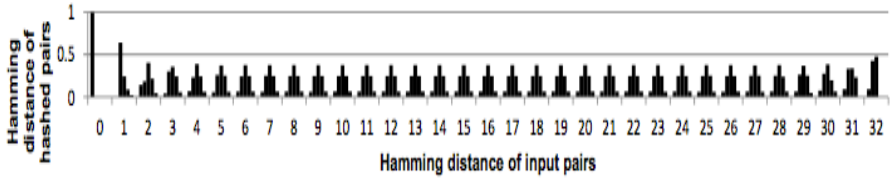
Results

- Prototype Implementation and evaluation on Altera DE4 board.



Step	Time (s)
Download data from FTP server	1.90
Check manufacturer certificate of network operator's public key K_O^+	3.33
Decrypt AES key K_{sym} using router's private key K_R^-	8.74
Decrypt package with AES key K_{sym}	7.73
Verify packet signature with network operator's public key K_O^+	3.92
Total	25.62
Total (no networking or certificate check)	20.39

- Hash function evaluation.



Conclusion and Future Work

- We have presented a system-level security design that ensures that hardware monitors on network processors can be programmed dynamically, while ensuring that attackers can not tamper with the monitoring system.

UMassAmherst

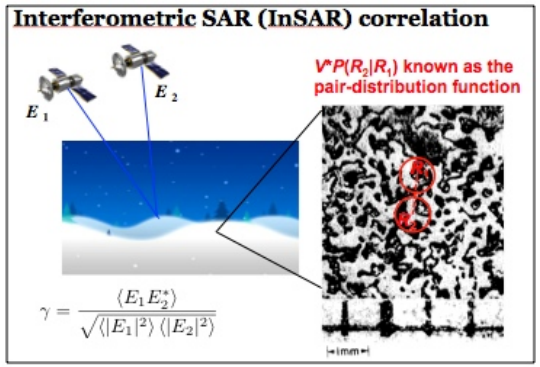
A DENSE-MEDIUM ELECTROMAGNETIC SCATTERING MODEL OF INSAR CORRELATION WITH ITS APPLICATION TO SNOW CHARACTERISTICS RETRIEVAL

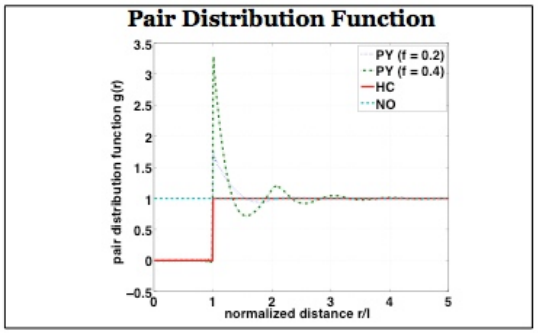
Yang Lei, Advisor: Prof. Paul Siqueira

Motivation

- Snow characteristics, such as Snow Water Equivalent (SWE) and snow grain size, are essential to monitor the global hydrological cycle and thus an indicator of climate change.
- In this work, an InSAR scattering model is derived for dense medium such as snow considering the multiple scattering effect through the use of Foldy-Lax equations and Quasi-Crystalline Approximation (QCA) and by incorporating the Percus-Yevick pair distribution function

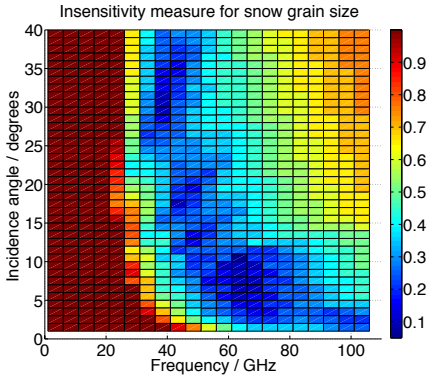
Technical Approach



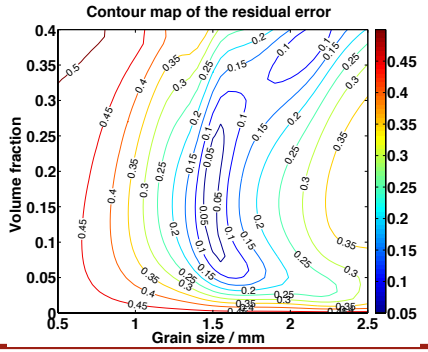


Results

Analysis



Snow Inversion



Conclusion and Future Work

An electromagnetic InSAR scattering model is derived for dense medium like snow. An inversion approach is developed to retrieve snow grain size and volume fraction/SWE and simulated validation results are illustrated. Future work entails the ground validation of the inversion approach.

UMassAmherst

Parameter Estimation via K-Median Clustering

Dian Mo, Advisor: Prof. Marco F Duarte

Motivation

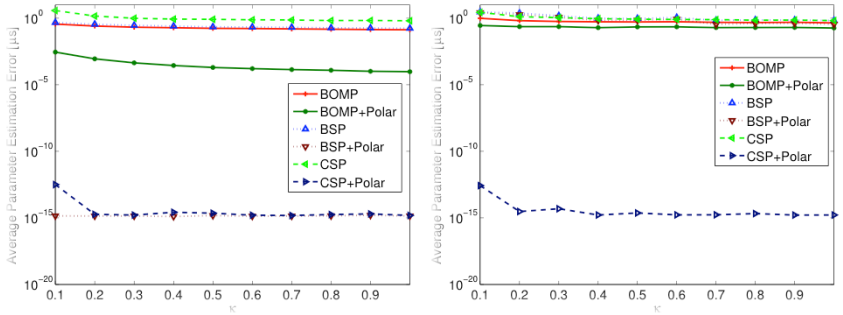
- Compressive sensing has been extended from signal recovery to parameter estimation
- Existing method to solve the coherence problem in parameter estimation requires additional setting
- The error guarantees result from CS algorithms has limit impact in parameter estimation

Technical Approach

- Observed signal is the mixture of parametric signals with unknown parameter
- Observation signal has sparse representation by designing the parametric dictionary
- The goal of existing parameter estimation algorithms is to accurately estimate the local maxima of proxy
- Sparse approximation find the closest vector to proxy/ input in EMD−sense, similar to hard thresholding for Euclidean distance
- EMD-closest sparse vector obtained by “partitioning” entries of proxy into K clusters by median proximity
- Nonzero entries correspond to centroids of clusters their values correspond to cluster sums of values
- Obtain EMD-based sparse approximation by finding set of K indices that minimize the clustering cost

Results

- K-median clustering can be applied for purposes of EMD-based sparse approximation
- Performance guarantees for EMD-based parameter estimation rely on the correlation function and cumulative correlation function
- Theorem and experiments show that estimating error has relationship with the minimum separation, off-bound distance and dynamic range of component magnitude
- Clustering method have comparable performance on time delay estimation as existing band−exclusion methods when its parameter is optimized



Conclusion and Future Work

- K-median clustering can be used to solve the coherence directly
- Clustering method provide EMD guarantees on the estimation error

UMassAmherst

Power-Optimized Temperature-Distributed Digital Data Link

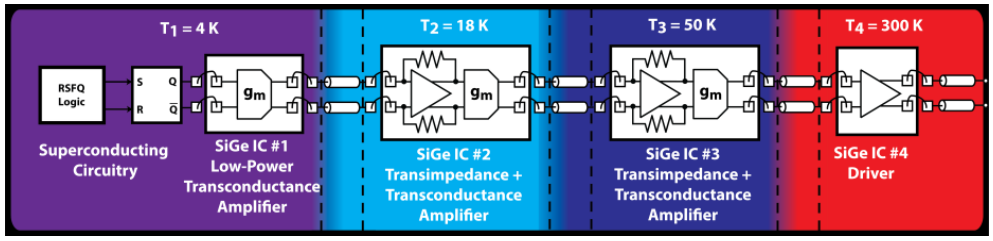
Prasana Ravindran Faculty Advisor : Prof. Joseph Bardin

Motivation

Nominal superconductor semiconductor based computational systems are able to leverage the fast operating speeds and low switching energy of superconducting logic and the high integration capacity of modern day FPGAs, but an efficient high bandwidth interface is not readily available. The challenge in building an efficient low power interface between 4 K logic and room temperature electronics lie in being able maintain a sufficient signal to noise ratio while achieving an acceptable bit-error rate.

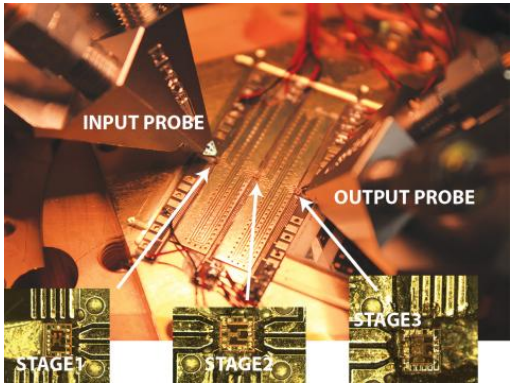
Technical Approach

Cold amplification is a natural solution to this problem, from a noise perspective one would push the amplification down to the lowest possible temperature, while from the point-of-view of minimizing power consumption, one would place the amplifier on a warmer temperature. An optimum approach to balance these divergent electrical and thermal requirements is to distribute the gain the power consumption over the 4 K -300 K temperature range.

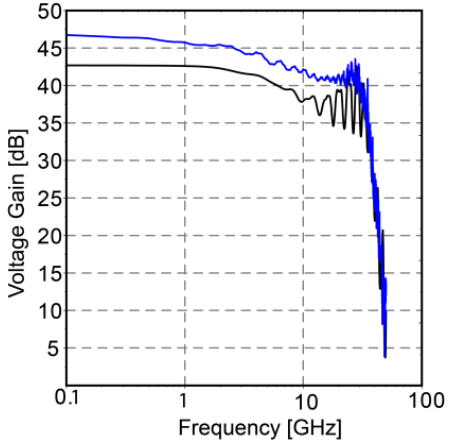


Block Diagram Of The Hybrid Temperature Heterogeneous Data Link

Link Results



a) Assembled link tested at 6 K



b) Blue line is measurement and black is the simulation

Power Consumption Analysis

	Temp	Power	Factor	Equiv. 300 K Power
STAGE 1	4 K	140 uW	3000	0.42 W
STAGE 2	18 K	1.8 mW	300	0.54 W
STAGE 3	50 K	18 mW	50	0.90 W

Conclusion and Future Work

- BW sufficient for > 30 Gbps
- Equivalent power consumption is < 1.9 W
- Future work involves demonstration of the full hybrid superconductor/semiconductor link, and BER measurements

UMassAmherst

Simultaneous Clustering & Embedding for Multiple Intimate Mixtures

Arun M Saranathan, Advisor: Prof. Mario Parente

Motivation

- Intimate Mixtures in hyperspectral images can be modeled as manifolds
- Since images often contain multiple mixtures we need manifold clustering and embedding techniques that can simultaneously ***classify*** the different mixtures present in the scene and ***embed*** them successfully in an appropriate lower dimension.

Technical Approach

- We present a scheme that preserves the objective of a classic embedding :-

$$J_1 = \underset{R}{\operatorname{argmin}} \, ||X - XR||_F^2 + \left|\left|\mathbf{1}^T R - \mathbf{1}^T\right|\right|_F^2$$
$$R_{ij} = 0; if\ i\ \&j\ are\ not\ neighbors$$

- while simultaneously ensuring that the columns of R can be clustered by using a kernel k-Means. The kernel k-Means objective is expressed using it's NNMF based analogue: -

$$J_2 = \underset{R,H\geq 0}{\min} \, ||W - HH^T||_F^2$$

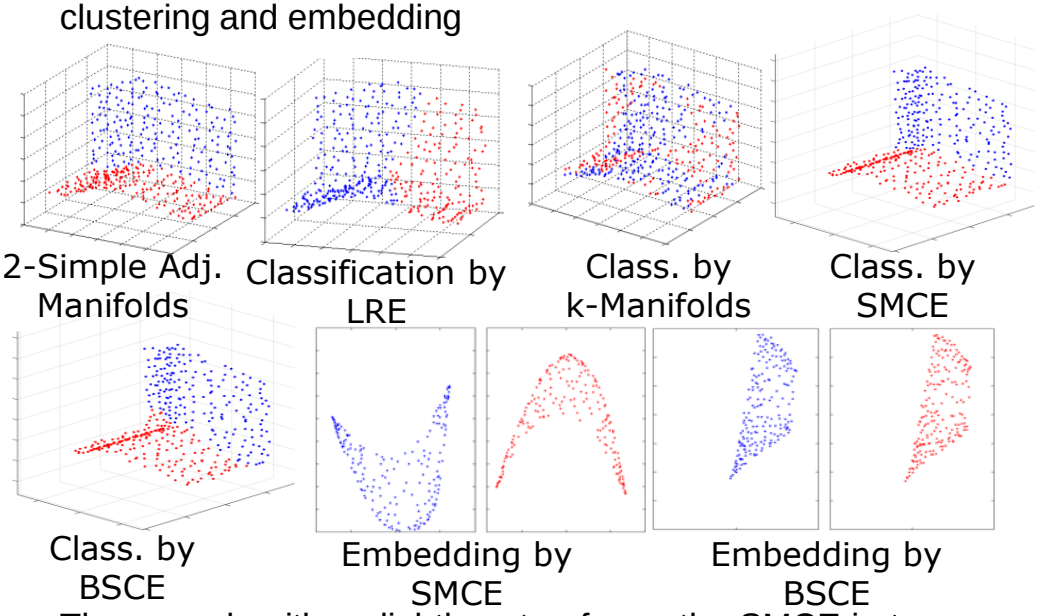
- leading to an overall objective function of: -

$$J = \underset{R,H\geq 0}{\operatorname{argmin}} \, ||X - XR||_F^2 + \lambda \left|\left|\mathbf{1}^T R - \mathbf{1}^T\right|\right|_F^2 + \mu||R^T R - HH^T||_F^2$$

- The overall objective function can the be minimized using the gradient descent technique with multiplicative updates.

Results

- In general the block-scheme for embedding and clustering outperforms it's closest competitors in terms of both clustering and embedding



- The new algorithm slightly outperforms the SMCE in terms of the classification but the embeddings from the new algorithm are far closer to the expected embeddings compared than the ones from SMCE.

Conclusion and Future Work

- Drop the positivity constraint on R in J to generate affine rather than convex embeddings to improve the embeddings at the corners.
- Replace kernel k-Means in J by the analogue of a better classification techniques such as N-Cuts.

UMassAmherst

Diagnostics for soil-transmitted helminths

Akshaya Shanmugam, Advisor: Raffi V. Aroian (UMass Med School), Christopher D. Salthouse

Motivation

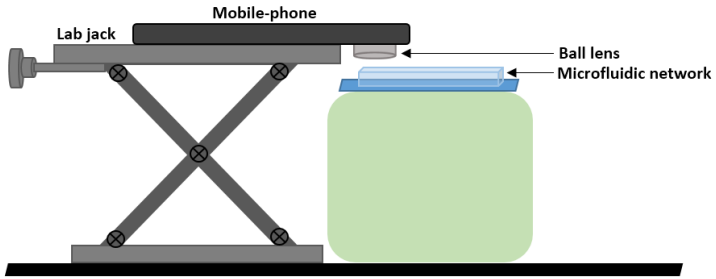
Soil-transmitted helminths (STH) are among the most common infections that affect poor and deprived communities. Traditional screening techniques pose certain challenges to the eradication of infection within a population. The screening technique proposed in this paper overcomes these challenges by offering high throughput screening at low costs.

Technical Approach

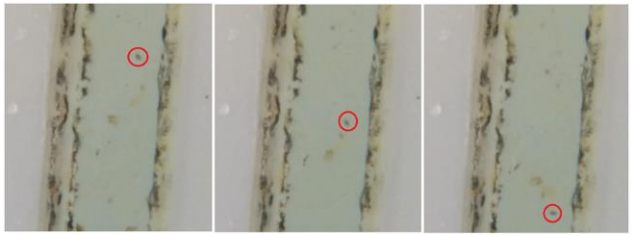
Traditionally, STH diagnosis involves the analysis of a stool smear under a microscope. In this work, the microscope is replaced by a mobile-phone microscope to reduce cost, screening time, and resources required for screening. During screening, the stool sample will be diluted and injected into a microfluidic network using a syringe. The microfluidic device will be held under the camera of the mobile-phone using a simple mechanical holder. A video will be recorded when the sample is injected and analyzed to detect STH eggs.

Results

Imaging set-up



Sample detection



The capability of the proposed technique was demonstrated by detecting whipworm eggs in mice feces. Figures show the proposed imaging set-up and frames from the captured video. The red circles highlight the whipworm eggs in each frame.

Conclusion and Future Work

The proposed technique reduces screening time by 85% and removes the need for an on-site technician. To improve the system further, an app to perform real time image processing for STH egg detection will be implemented.

UMassAmherst

Leveraging an Ephemeral Key to Obtain Everlasting Security in Wireless Environments

Azadeh Sheikholeslami, Advisors: Prof. Dennis Goeckel, Prof Hossein Pishro-Nik

Motivation

Everlasting secrecy:

- We are interested in keeping something secret forever.
- A challenge of cryptography (e.g. the VENONA project) is that recorded messages can be deciphered later.

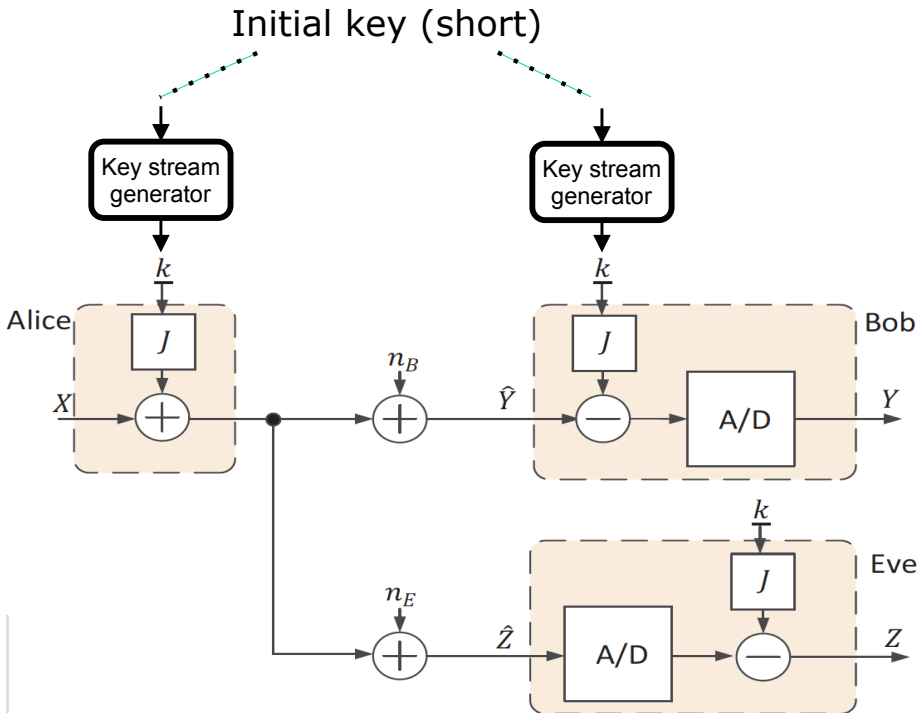
Technical Approach

- Alice and Bob share a short "ephemeral" cryptographic key.
- By employing a cryptographic stream-cipher generation method, this initial key is used to obtain a long key sequence.
- Alice adds a random jamming signal with large variations based on the key to the message.
- Bob uses key to cancel the effect of jamming before A/D conversion.
- Eve has to wait to obtain the key after completion of transmission.

Eve's strategy:

- Do not change span of her A/D ➡ A/D overflows
- Enlarge span of A/D to prevent overflows ➡ degrade resolution

Eve loses information



Conclusion and Future Work

- We have proposed a technique to convert ephemeral "cheap" cryptographic key bits to "expensive" information-theoretically secure bits to achieve everlasting security.
- The numerical results show that this method can provide robust secrecy even in the case that the eavesdropper has perfect access to the output of the transmitter's radio.
- For the future work we will consider this approach in a network setting.

UMassAmherst

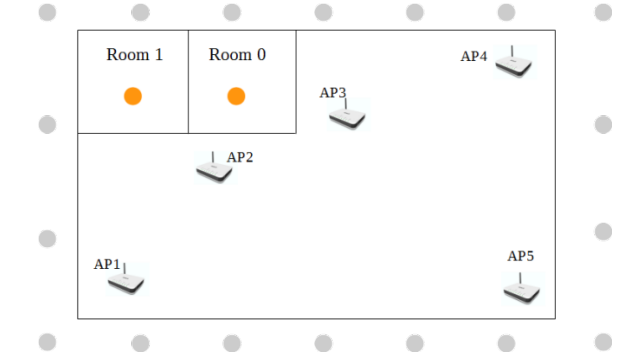
Determining the Originating Room of Wireless Transmissions using Exterior RSS Measurements

Tamara V. Sobers, Advisors: Prof. Dennis Goeckel & Prof. Patrick Kelly

Motivation

- Wireless Indoor Localization estimates where a device is located inside of a building using a radio map/dictionary.
- You cannot use an interior radio map to perform indoor localization if access to a building is not guaranteed.
- We use RSS measurements collected from the exterior of the building to perform indoor localization by estimating the indoor map.

Technical Approach



= Exterior Positions ● = Interior Room Map

- We use the distance from each exterior point to the center of the p^{th} room as features to estimate RSS measurements in room p
- Estimate the interior map using 4 methods for comparison: k-NN, weighted k-NN, k-NN with attenuation compensation and wk-NN with attenuation

Results

- Using the interior estimate, a Likelihood Ratio Test estimates whether the device was located in 1 of 2 rooms
- The experiment was performed in Marston Hall Rooms 128, 132, and 134 for different combinations of 2 room detection
- Data from Exterior Positions were collected in August 2014 and data from indoor test positions were collected over 10 days from Sept 2014 to Feb 2015.
- Estimation methods were compared to a "True" interior map that was generated by collecting data

	$H_1 = 132, H_0 = 128$	$H_1 = 128, H_0 = 134$	$H_1 = 132, H_0 = 134$
True	.0167	.0833	.4167
k-NN	.0083	.0833	.3917
wk-NN	.1667	.3667	.7917
A-k-NN	.25	.5	.4333
A-wk-NN	.25	.5	.2583

Conclusion and Future Work

- Initial results are promising but including attenuation in the estimate does not perform as well as expected due to faults in the experiment.
- We plan on improving the experimental design, extending room classification to multiple rooms, and will assume the device is unknown (unknown transmit power)

UMassAmherst

The making of a new numerical parallel library: the SPIKE-SMP banded system solver

Braegan Spring, Advisor: Prof. Eric Polizzi

Motivation

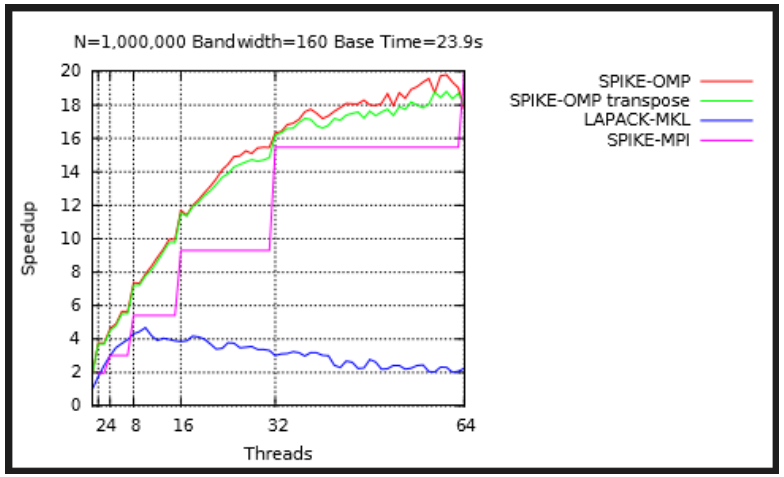
- Desktop, workstations CPU's have many cores already, trend continuing
- Exploiting parallelism can be hard
- Use of Linear Algebra subroutines already popular
- Therefore, an easy (nearly) drop in replacement for a matrix solver would be useful
- Banded matrices are particularly amenable to parallelism

Technical Approach

- Implemented the (preexisting) SPIKE recursive algorithm using standard technologies
  - Domain decomposition approach – break banded matrix up along the diagonal. (Matrix is factorized into a matrix composed of decoupled sub-matrices along the diagonal, and the 'spike matrix' which represents communication between domains)
    - Ax=DSx=y : Find x
  - All parallelism is performed by OpenMP (built in to modern FORTRAN compilers)
  - Follows the standard LAPACK naming conventions
- Designed Transpose Spike algorithm
  - Reuse the DS factorization
  - Transpose S matrix has an exploitable geometry

Results

- Good scalability on shared memory machines
  - Benchmarked up to 20X single threaded native LAPACK on large machine
- Allows user to use their own single-threaded code, call SPIKE to provide parallelism



Future Work

Include SPIKE into Prof. Polizzi's FEAST eigenvalue solver

Investigate possible strategy to improve stability for less well conditioned matrices

UMassAmherst

GreenSort: An Energy-agile Distributed Sorting System

Supreeth Subramanya, Advisor: Prof. David Irwin

Motivation

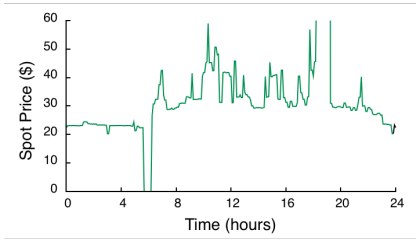
- With gains from energy-efficiency plateauing, how do we improve the impact of energy significantly?
- We introduce a new metric ***Energy-agility***, to measure the ability to adapt applications to dynamic power variations

Technical Approach

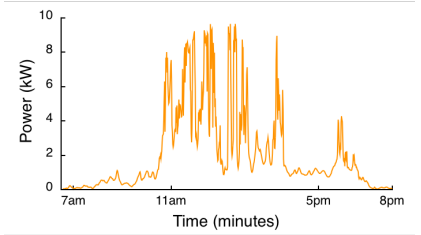
- We define & describe *energy-agility* as a performance metric
- ***How to design energy-agile systems?*** We analyze mechanisms (active and inactive power-capping) and policies (prioritize, blink, or round-robin) across the design space
- In this work, we ***focus*** on long-running, massively-parallel, big-data jobs that are common in datacenters
- We design ***GreenSort***, an energy-agile distributed sorting system that is constrained by the input power signal p(t)
- We implement and deploy GreenSort on the ***MGHPCC*** datacenter, and evaluate all three energy-agile policies

Results and Conclusions

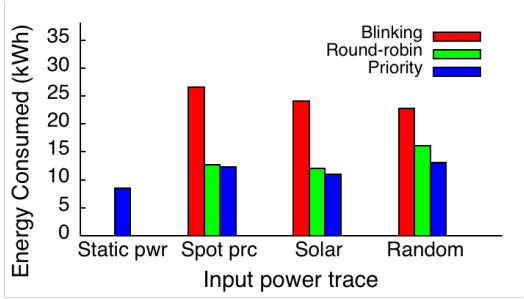
Energy-agility of GreenSort with different policies for real-world signals



(a) Electricity spot price



(b) Solar power input



(c) Energy-agility of GreenSort

- We distinguish energy-agility from energy-efficiency, and explore all the parameters that affect agility
- Variations in power increase both time and energy required to complete a task: *real-time electricity prices should be >31% lower than fixed prices to warrant opting into using them*
- ***Many of today's servers lack mechanisms to support agility***

UMassAmherst

Exploring Economic Dynamics in an Internet with Service Choices

Thiago Teixeira, Advisor: Prof. Tilman Wolf

Motivation

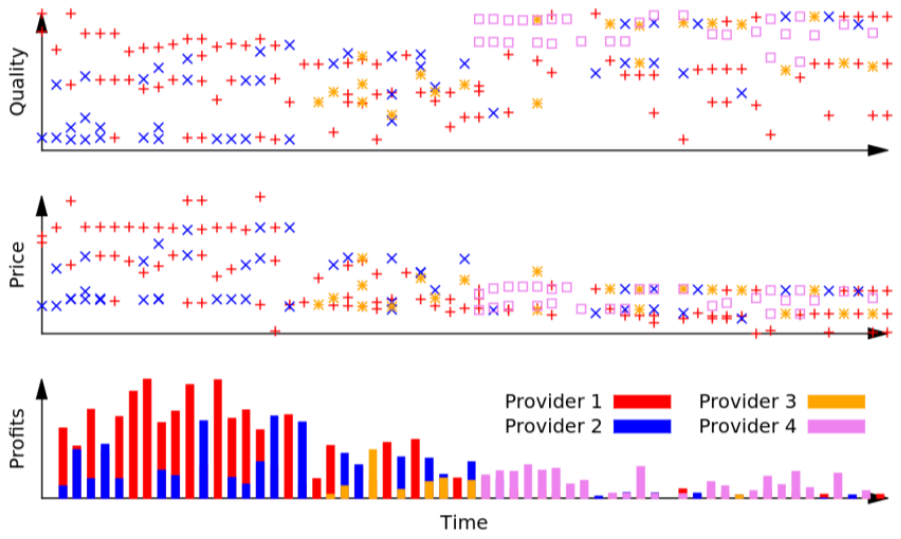
- In today's Internet, most ISPs offer end-users only simple and coarse price choices (flat rate).
- Consequently, users have no control over what happens with their traffic inside the network.
- A number of innovative technologies have been addressing this shortcoming.

Technical Approach

- New technologies and network architectures enables fine-grained and dynamic economic relationships between users and providers.
- We developed an agent-based simulation to understand how these new economic interactions would affect the relationship between customers and providers in a service-oriented Internet.
- Our network services are characterized by ***quality*** (i.e., throughput, delay, jitter, packet loss) and ***price***.
- Consumers not only consider price, but the overall set of attributes that maximize their benefits.
- Provider offers are characterized by a set of attributes that are updated after each interaction.
- Services are offered in the marketplace, which acts as a trusted entity and is responsible for clearing the market.

Results

- The following graphs show the evolution of price and quality over time, increasing competition (as more providers enter the market) and innovative services.



Conclusion and Future Work

- In an oligopoly scenario with innovative network services, providers need to innovate in order to survive in the new market by improving end-user experience.

UMassAmherst

Monte Carlo study of the effects of nanostructuring on thermal transport in SiGe Nanowires

Meenakshi Upadhyaya, Advisor: Prof. Zlatan Aksamija

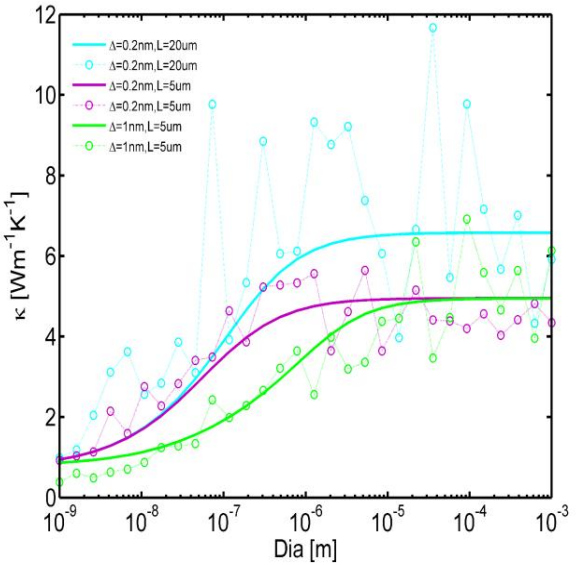
Motivation

- High performance thermoelectric energy conversion has been hindered due to strongly correlated thermoelectric properties.
- The simple approach to improving efficiency is to reduce thermal transport by means of nanostructuring and alloying.

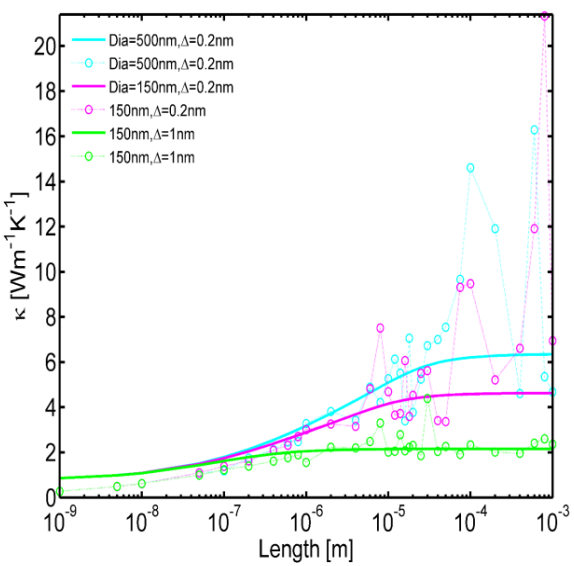
Problem & Approach

- Thermal conductivity in SiGe nanowires has a weak diameter dependence indicating that scattering of phonons at the nanowire boundary and strong mass difference scattering of phonons with the constituent components of the alloy do not add together according to Matthiessens rule.
- This is because the effect of alloying and boundary scattering are not independent and for a phonon to scatter at the rough boundary, it must not suffer a collision due to mass-difference or anharmonic interactions before reaching the boundary.
- The Monte Carlo technique is used to obtain the phonon lifetimes from all the scattering processes and the minimum of all the lifetimes is considered to compute the conductivity.
- $k = \Sigma c_{ph,i} v_{g,n,i}^2 \frac{\Lambda_i}{|v_{g,i}|}$

Results



Thermal conductivity as a function of diameter. The solid lines represent the BTE results and dashed lines represent the Monte Carlo results. The diameter dependence is weak due to strong intrinsic scattering.



Thermal conductivity as a function of length. The solid lines represent the BTE results and dashed lines represent the Monte Carlo results. We observe a gradual transition from the quasi ballistic to diffusive regime.

Conclusion

- The combination of alloying and boundary scattering leads to a thermal conductivity lower than that achievable by any one of the two processes.
- Alloy scattering reduces the effect of boundaries by up to a factor of two leading to a weak sub-linear diameter dependence.
- The lower part of the phonon spectrum remains unaffected and these long wavelength phonons lead to ballistic thermal conduction over 10 μm.

UMassAmherst

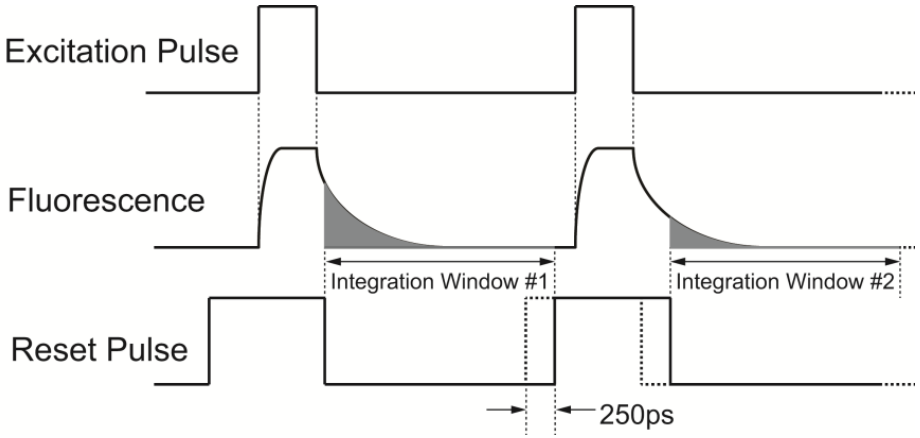
Novel Instruments for Fluorescence Lifetime Measurement

Hongtao Wang, Advisor: Prof. Christopher Salthouse

Motivation

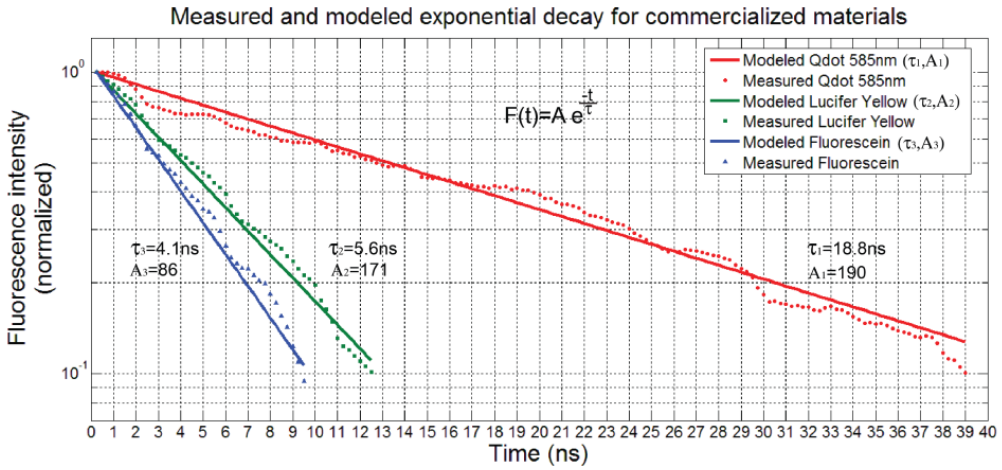
- Building a novel fluorometer to accurately measure the lifetime of fluorescent chemicals.
- Portable, low-cost, high sensitivity, no optics.
- Cappable of sensing fluorecence decay with several nanoseconds to tens of nanoseconds time constant.

Technical Approach



- Integrate the amount of light in a time window and shift the window linearly with a sub-nanosecond step.
- The integration of the exponential decay possesses the same time constant. Can be extracted by fitting.
- Electronic shutter can separate the excitation light and the emission light.

Results



- Measured 3 commercial fluorophores with well known lifetimes. All measurement results confirm the reported values.
- Measured water solution of one type of fluorophore in different concentrations. The detection limit of the instrument is 1 order of magnitude lower than the frequency method.

Conclusion and Future Work

- Our time-domain fluorometer is low-cost (<250 USD) and portable (~iPhone 4).
- LED excitation source feature provides arbitrary excitation wavelength options.
- We are designing IC chips that can realize the system.

UMassAmherst

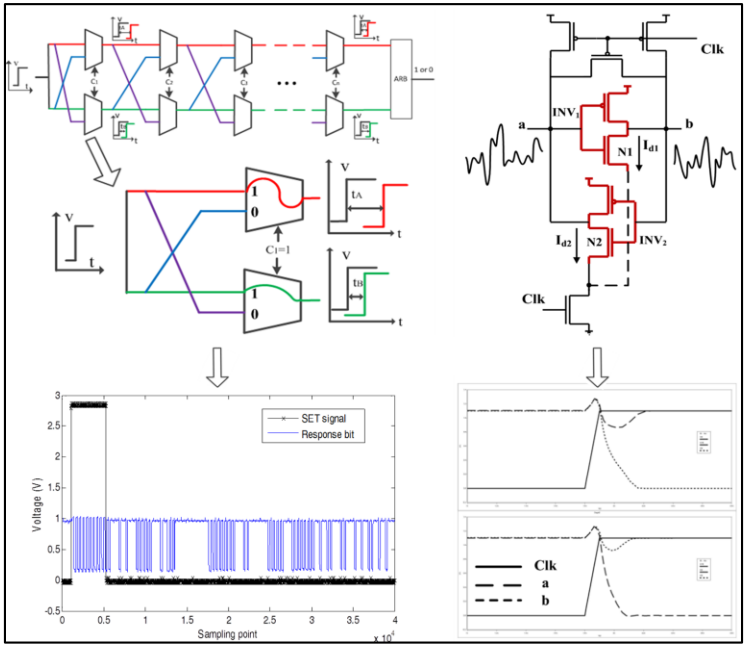
Secure Computation in CMOS

Xiaolin Xu, Advisor: Prof. Wayne Burleson

Motivation

- Modern cryptographic and security schemes are built on the concept of a secret key/function. This forces current hardware to contain a piece of digital information, and must remain, unknown to the adversary. Lightweight engineering solutions based on hardware security favor practical applications like implantable medical devices, and transportation payment systems.

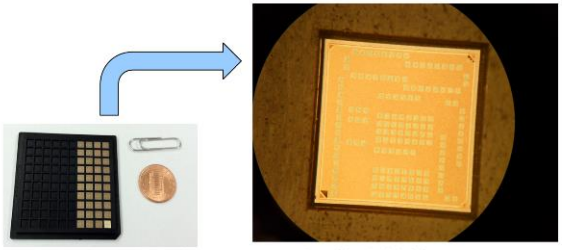
Technical Approach



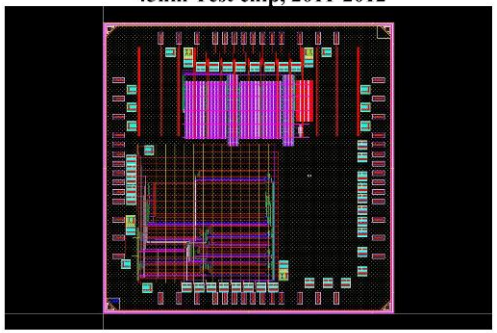
- Secure key-storage based on lightweight PUF;
- Secure and lightweight random number generation based on TRNG.

Results

Silicon Implementation



45nm Test chip, 2011-2012



32nm Test chip, 2014-2015

- 45nm test chip with reliable PUF, thermal sensor, etc;
- 32nm test chip with TRNG, PUF ECC.

Conclusion and Future Work

- Proposed some enhancements for IMD and transportation applications;
- Looking for Stronger security architectures and implementing new attacking methods to reversely improve these functions.

UMassAmherst

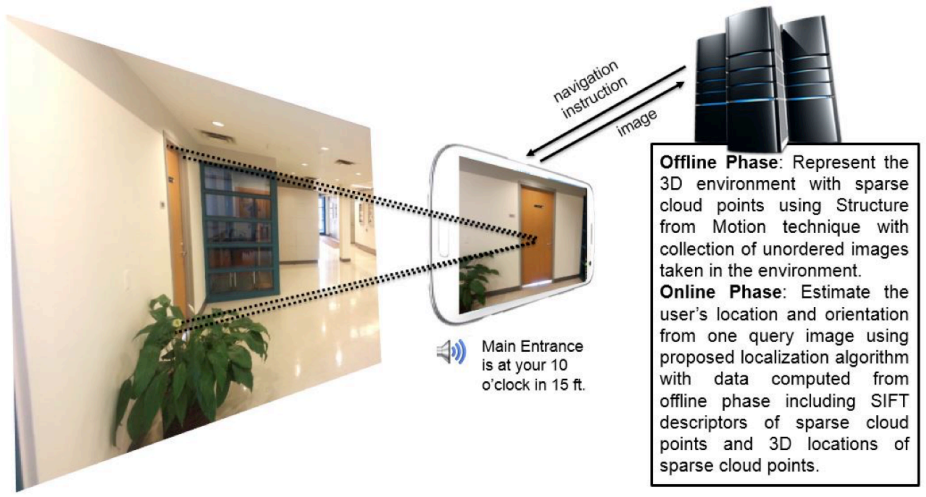
Ubiquitous Vision-based Localization Algorithm using a Smartphone

Zhuorui Yang, Advisor: Prof. Aura Ganz

Motivation

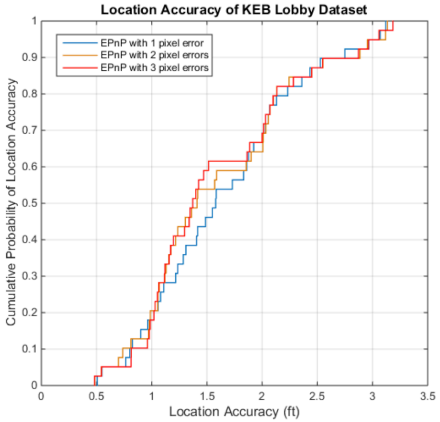
- Vision-based localization technologies hold promise for many ambient intelligence applications, including navigational assistance for individuals with wayfinding difficulties, especially for the visually impaired.

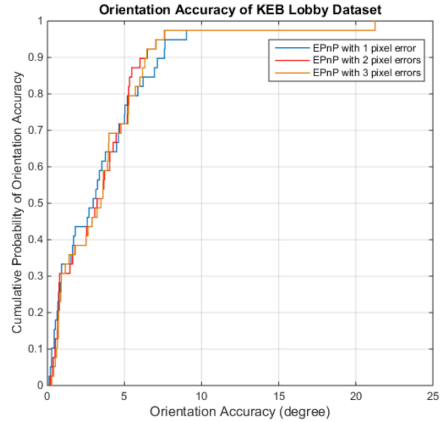
Technical Approach



Offline Phase: Represent the 3D environment with sparse cloud points using Structure from Motion technique with collection of unordered images taken in the environment.
Online Phase: Estimate the user's location and orientation from one query image using proposed localization algorithm with data computed from offline phase including SIFT descriptors of sparse cloud points and 3D locations of sparse cloud points.

Results





Conclusion and Future Work

- From our study, we have achieved mean location accuracy as good as 1.6 ft, mean orientation accuracy less than 3.5 degree and real-time performance at the same time. We are also working on building a confidence metrics to improve the robustness, etc.

UMassAmherst

Scalable Nonnegative Matrix Factorization with Block-wise Updates

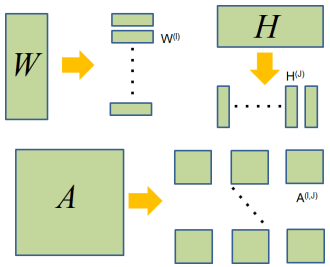
Jiangtao Yin, Advisor: Prof. Lixin Gao

Motivation

- Nonnegative Matrix Factorization (NMF) is a popular tool to uncover latent relationships in matrices
- NMF factorizes matrix A into two matrices W and H, $A \approx WH$, minimizing a loss function, $L(W,H)=||A-WH||$
- Many applications (on big data): computer vision, recommendation systems, document clustering, etc.

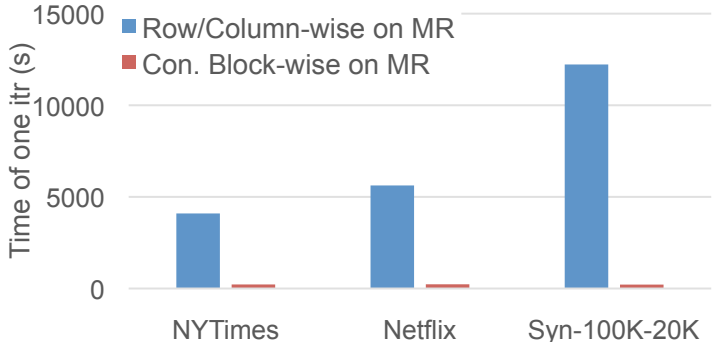
Technical Approach

- A novel divide-and-conquer method
  - Split W and H into blocks along the short dimension to scale NMF to million-by-million matrices
  - Partition A into corresponding blocks

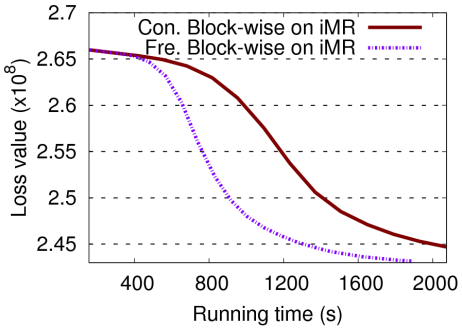


- Block-wise Updates: update one block at a time instead of the entire factor matrix
- Flexible Update Scheme: block-wise updates can update blocks of a factor matrix independently

Results



The implementation of concurrent block-wise updates is 19x - 57x faster than that of traditional updates



- Frequent block-wise updates always converge faster than concurrent block-wise updates

Conclusion and Future Work

- Propose a new form of updates, block-wise updates, for NMF
- Block-wise updates enable efficient distributed implementation
- Achieve up to two orders of magnitude speedup compared with that of traditional updates